Banned Tracking Technology Use Among Medical Device, Pharmacy, and Hospital Webforms: A Cross-Sectional Study

Andrea Downing, Jill Holdren

Submitted to: Journal of Medical Internet Research
on: March 15, 2024

Table of Contents

Banned Tracking Technology Use Among Medical Device, Pharmacy, and Hospital Webforms: A Cross-Sectional Study

Andrea Downing[1*] BBA, BA; Jill Holdren[1*] MSc

[1]The Light Collective Eugene US
[*]these authors contributed equally

Corresponding Author:
Andrea Downing BBA, BA
The Light Collective
1711 Willamette St #301
Eugene
US

Abstract

Background: Tracking technologies are frequently employed to gather and examine data regarding user interactions with websites or mobile applications of regulated health-related entities. These technologies then illegally share user data with third parties that use it to target ads to patients across social media platforms. This collection and sharing constitutes a data leak of massive proportions. Specifically, some pharmacies, medical device companies, and hospitals utilize banned tracking or surveillance technologies on their websites in a way that exposes patients' prescriptions, medical device information, doctor appointments and contact details to third parties.

Objective: This study aimed to assess the use of prohibited tracking technologies on unauthenticated URL's within three types of entities: pharmacies, medical companies, and health systems.

Methods: We identified the largest-by-revenue medical device companies, pharmacies, and hospitals in the United States, using a scanning tool we developed based on existing open source software to detect the presence or absence of five banned tracking technologies on a sample of them.

Results: In total, we included 341 URLs associated with three different types of HIPAA covered entities in our scan sample. Medical device company (n= 147) webpages comprised 43.1% of our overall sample. Pharmacy webpages (n=96) comprised 28.2% of our sample, and hospitals/health system URLs (n=98) comprised 28.7% of our sample. 63.9% of the medical device company URLs scanned contained at least one banned surveillance technology. 59.2% of pharmacy URLs scanned had at least one banned surveillance technology installed. 59.8% out of hospital URLs scanned contained at least one banned surveillance tracker.

The most common tracker found on medical device company sample was Google Audience (39.5%), followed closely by Facebook Pixel (36.1%)

There were a number of device companies, pharmacies, and hospitals scanned that had none of the banned trackers. n=53 URLs or 36.1% did not have any banned trackers identified. 40.8% (44) of pharmacies did not have any trackers. 67.0% of hospital URLs scanned did not have any trackers identified.

Conclusions: This study demonstrates the presence of health trackers on many health-related sites despite the laws that prohibit them, and further examines the ways PHI may be shared with social media platforms or third parties via unauthenticated landing pages. Future studies are needed to assess the impact of leaking sensitive data belonging to millions of patients to third party vendors. Clinical Trial: n/a

(JMIR Preprints 15/03/2024:55646)
DOI: https://doi.org/10.2196/preprints.55646

Preprint Settings

1) Would you like to publish your submitted manuscript as preprint?

✓ **Please make my preprint PDF available to anyone at any time (recommended).**
Please make my preprint PDF available only to logged-in users; I understand that my title and abstract will remain visible to all users.
Only make the preprint title and abstract visible.
No, I do not wish to publish my submitted manuscript as a preprint.

2) If accepted for publication in a JMIR journal, would you like the PDF to be visible to the public?

✓ **Yes, please make my accepted manuscript PDF available to anyone at any time (Recommended).**
Yes, but please make my accepted manuscript PDF available only to logged-in users; I understand that the title and abstract will remain v
Yes, but only make the title and abstract visible (see Important note, above). I understand that if I later pay to participate in <a href="http

Original Manuscript

Banned Tracking Technology Use Among Medical Device, Pharmacy, and Hospital Webforms: A Cross-Sectional Study

Co-Authors: Andrea Downing, Jill Holdren, Marlena Murphy, Christine Von Raesfeld, Ella Balasa, Michael Mittelman, Dr. Erik Perakslis, Dr. Cait Desroches

Abstract

Background: Tracking technologies are frequently employed to gather and examine data regarding user interactions with websites or mobile applications of regulated health-related entities. These technologies then illegally share user data with third parties that use it to target ads to patients across social media platforms. This collection and sharing constitutes a data leak of massive proportions. Specifically, some pharmacies, medical device companies, and hospitals utilize banned tracking or surveillance technologies on their websites in a way that exposes patients' prescriptions, medical device information, doctor appointments and contact details to third parties.

Objective: This study aimed to assess the use of prohibited tracking technologies on unauthenticated URL's within three types of entities: pharmacies, medical companies, and health systems.

Methods: We identified the largest-by-revenue medical device companies, pharmacies, and hospitals in the United States, using a scanning tool we developed based on existing open source software to detect the presence or absence of five banned tracking technologies on a sample of them.

Results: In total, we included 341 URLs associated with three different types of HIPAA covered entities in our scan sample. At least one form of banned tracking technology in 63.9% of the medical device company urls scanned, 54.2% of pharmacy urls scanned, and 59.2% of the health system' URLs scanned. Overall 59.8% of all unauthenticated webforms scanned found at least one banned tracking technology. This study also found sites that were free of tracking technologies. 36.1% of medical device company websites, 45.8% of pharmacy websites, and 40.8% of hospital URLs did not have any banned trackers identified. Overall 40.2% of the unauthenticated webforms had no tracking technologies installed.

Conclusions: Our scans revealed the presence of banned tracking technology on URLs associated with all three types of entities. Despite liability risks, patient safety risks, and a definitive ban on surveillance technologies for unauthenticated webpages, this study has found significant use of tracking technologies on HIPAA Covered entities' websites between 2024-2024. These specific tracking technologies were installed on unauthenticated webpages which gather PHI from patients.

Keywords: Surveillance tracking technology; patient safety; health privacy; HIPAA

Introduction

Snippets of code can be added to any website to collect and analyze information about users for advertising or marketing. For example, Meta Pixel is a tracking technology that many websites install to share data back with about users' activity. The presence of these trackers on HIPAA covered websites is now considered a privacy breach by the U.S. Department of Health and Human Services and the Federal Trade Commission[1].[1]

In February 2022, a proof-of-concept study led by patient advocates showed the privacy and policy implications of tracking technologies for 5 diagnostic testing companies that were sharing data with Facebook without consent[2].[2] A subsequent investigation reproduced the study method with authenticated patient portals, showing that sensitive health and legally-protected information was being shared with Meta (the parent company of Facebook). Specifically, the study found that 30 of the top 100 hospitals had shared protected health information (PHI) with Meta[3].[3] A third study found third-party tracking present on 98.6 percent of hospital websites, with transfers of PHI to large technology companies, social media companies, advertising firms, and data brokers[4].[4] By October 2022, the Emergency Care Research Institute (ECRI) issued a safety alert to approximately 5000 member hospitals warning about the leaking of PHI from hospital patient portals[5].[5]

By December 2022, a definitive ban on tracking technologies was issued by the Department of Health & Human Services (HHS).[6] This notice from the Office of Civil Rights included clear guidance and definitions for what constitutes an online tracking technology, and what constitutes a violation of HIPAA. Specifically, the notice stated regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules[6].

To date, there has not yet been an examination of tracking technology use on unauthenticated webforms, such as account creation, appointment request, and login pages. We set out to understand whether there are different types of covered entities who have banned tracking technologies on their websites, following the guidance issued. In theory, covered entities would be able to follow the guidance. Yet, we were interested to study and compare differences in use of these tracking technologies and find out if unauthentic webpages can share more about a patient than whether they visited a covered entity's website. Therefore this study set out to examine the extent of banned tracking technologies installed and still in use on a sample of unauthenticated web pages of U.S. hospitals, pharmacies, and medical device manufacturers, with a focus on webforms that may gather sensitive PHI.

1https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking

2Downing A, Perakslis E. Health advertising on Facebook: Privacy and policy considerations. Patterns (N Y). 2022 Aug 15;3(9):100561. doi: 10.1016/j.patter.2022.100561. PMID: 36124307; PMCID: PMC9481952.

3Feathers T, Fondrie-Teitler S, Waller A, Mattu S. Facebook is receiving sensitive medical information from hospital websites. STAT [serial on the Internet]. 2022 Jun 16 [cited 2023 Feb 9]. Available from: https://www.statnews.com/2022/06/16/facebook-meta-pixel-hospitals-data/

4 Friedman, Ari B et al. "Widespread Third-Party Tracking On Hospital Websites Poses Privacy Risks For Patients And Legal Liability For Hospitals." Health affairs (Project Hope) vol. 42,4 (2023): 508-515. doi:10.1377/hlthaff.2022.01205

5 ECRI Safety Alert, October 2022 https://medcitynews.com/uploads/2022/11/ECRI-Alert-View.pdf

6 https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html

Methods

Our patient-led team evaluated the use of third-party tracking technologies on a sample of US hospital, device, and pharmacy websites. We used a tracker identification tool to scan public, unauthenticated web pages for a pre-identified set of tracking technologies.

Dataset/Website Identification

The methodology focused on identifying websites associated with three types of entities that are covered in recent guidance on the use of third party trackers from HHS and the FTC: medical device companies, pharmacies, and hospitals. In order to narrow down our sample to a manageable size, we started with an established list of the top 100 medical device companies by market cap in 2022[7].[7] For Pharmacies we worked from an established list of the top pharmacies by revenue size [8].[8] Finally, for hospitals we worked from Becker's top 60 US hospitals by number of beds as a predefined list[9].[9]

The primary inclusion criteria for our analysis was unauthenticated web pages on which patients enter and submit contact details and/or some form of protected health information. To obtain URLs to scan, we manually searched websites from each list to identify whether URLs on our target list had the following types of unauthenticated web pages:

- Account Sign-Up Forms
- Device or Product Registration Pages
- Appointment Request Forms
- Patient Portal Login Pages

The reason for focusing on these types of webforms is that if third-party tracking code is installed on the specific types of pages listed above, sensitive information from the patient would be shared with third parties, depending on the type of tracking technology installed. Further, data in webforms are specific to the patient's unique identity and relationship with the health entity in a way that goes beyond viewing content of a webpage.

Our analysis excluded any links scanned that did not fit the definition of a covered entity under the ban on surveillance technologies as well as any links that were duplicates (Figure 1). Note that we did not scan all web pages that may meet criteria of an unauthenticated web page that collects personal information at every site.

Scanning Tool

The scan tool we utilized was developed using established open source methodologies that scan

7 "The 2022 Medtech Big 100: The world's largest medical device companies." Medical Design & Outsourcing, September 2022, https://www.medicaldesignandoutsourcing.com/2022-big-100/. Accessed May 2023.

8 Twenter, Paige. "15 biggest pharmacies by prescription revenue." *Becker's Hospital Review*, 13 April 2023, https://www.beckershospitalreview.com/pharmacy/15-biggest-pharmacies-by-prescription-revenue.html. Accessed 14 March 2024.

9 Behm, Carly, et al. "100 largest hospitals and health systems in the US | 2023." Becker's Hospital Review, 15 December 2023, https://www.beckershospitalreview.com/rankings-and-ratings/100-largest-hospitals-and-health-systems-in-the-us-2023.html . Accessed 12 March 2024.

URLs to look for certain surveillance technologies[10].[10] Over the previous decade and through extensive studies, Princeton researchers identified several privacy-invading technologies, including canvas fingerprinting[11].[11] In this study, , the team assessed the number and types of third party tracking on the websites in the sample by scanning the link for installations of ad trackers, fingerprinting, session recording, retargeting audiences, or Meta Pixel [12] **(Table1).**[12]

Table 1. Types of tracking technologies studied.

Tracker Type	Description
Ad Trackers	Ad trackers, often in the form of JavaScript scripts or tiny 1px by 1px web beacons, collect information about users' online activities for advertising purposes. These beacons, placed on websites, enable third parties to track when a user visits a site, record their IP address, and identify the browser type used, aiding in targeted advertising strategies.
3rd Party Cookies	Third-party cookies consist of a small piece of data stored in a web browser by tracking companies upon visiting a website. This data, often a unique number or string of characters, serves to identify visitors on other websites containing tracking code from the same company. These cookies are employed by numerous companies to compile information about users, enabling the delivery of personalized ads tailored to their online behavior.
Canvas Fingerprinting	Canvas Fingerprinting identifies browsers without cookies by drawing shapes and text on webpages, detecting unique rendering differences, even when cookies are blocked.
Session Recording	Session recording technology captures and records user behavior on a webpage, including mouse movements, clicks, scrolling, and text entered in forms, regardless of submission.
Key Logging	Key logging involves monitoring text input on a webpage prior to submission, used for various purposes like linking anonymous web users to their real identities. Key logging also facilitates features like autocomplete, but the intent behind a website's use of key logging cannot always be discerned.
Facebook Pixel	Facebook Pixel is a snippet of JavaScript code that loads a small library of functions you can use to track Facebook ad-driven visitor activity on your website. It relies on

10 Mattu, Surya, and Aaron Sankin. “How We Built a Real-time Privacy Inspector – The Markup.” The Markup, 22 September 2020, https://themarkup.org/blacklight/2020/09/22/how-we-built-a-real-time-privacy-inspector. Accessed 23 February 2024.

11 Englehardt, Steven, and Arvind Narayanan. "Online tracking: A 1-million-site measurement and analysis." *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. 2016.

12 Englehardt, Steven, et al. "Cookies that give you away: The surveillance implications of web tracking." *Proceedings of the 24th International Conference on World Wide Web*. 2015.

	Facebook cookies, which enable us to match your website visitors to their respective Facebook User accounts.
Google Audience	Google Audiences track a users' activity using Google products and browsing behavior of third-party websites, or estimated based on content certain groups of people are likely to be interested in.

Third-party tracking was then assessed on a rolling basis over a six-month period (August 1st, 2023-March 15th, 2024), following the OCR Guidance issued in December of 2022. Each scan produced a timestamped report of the results for a given URL during the study period. Results of each scan were summed and categorized by type of tracker and type of entity.

While we also scanned each URL for third party cookies and ad trackers, we did not focus on these results in this paper as it is not within the scope of this study to determine which of those cookies and ad trackers are functional (necessary for the functioning of the page) and which are non-functional.

Validation

We used a secondary validation method in order to compare/ reproduce the results by scanning a random sample of links using Mozilla's Privacy Badger [13].[13] We also checked to ensure that the scanned links met the exact criteria for inclusion in the study.

During the validation phase, we determined that the team scanned additional sites (n=156) that ultimately did not meet selection and/or eligibility criteria during the process. We have excluded these results from the analysis.

Results

The overall results showed that a significant number of HIPAA covered entities' websites still contained banned surveillance technologies at the time of the scans. There were also a significant number of websites that were completely free of trackers without any apparent impact on function of the website

We analyzed a sample comprising URLs from various entities within the healthcare sector. Our sample included 147 medical device company websites (43.1% of the total sample), 96 pharmacy websites (28.2% of the total sample), and 98 hospital or health system URLs (28.7% of the total sample), totaling 341 individual URLs.

Our analysis revealed the presence of banned tracking technology on URLs associated with all three types of entities **(Table 2)**. Specifically, we identified at least one form of banned tracking technology in (n=94) 63.9% of the medical device company urls scanned, (n=52) 59.2% of pharmacy urls scanned, and (n-58) 59.2% of the health system' URLs scanned. Overall 59.8% of all unauthenticated webforms scanned had at least one banned tracking technology.

Our analysis also found entities free of all five banned tracking technologies. Specifically, (n=53) 36.1% of medical device company websites, (n=44) 45.8% of pharmacy websites, and (n=40) 40.2%

13 Privacy Badger, https://privacybadger.org. Accessed 23 February 2023.

of hospital URLs did not have any banned trackers identified. Overall 40.2% of the unauthenticated webforms scanned were free of tracking technologies.

Table 2. Presence and absence of banned trackers on a sample of HIPAA covered entities (n=341).

Entity Type	Total Scanned	URLs with ≥1 Banned Tracker	≥1 Banned Tracker (%)	N=0 Banned Trackers	0 Banned Trackers (%)
Device Companies	147	94	(63.9%)	53	(36.1%)
Pharmacies	96	52	(54.2%)	44	(45.8%)
Hospitals	98	58	(59.2%)	40	(40.8%)
Total	341	204	(59.8%)	137	(40.2%)

We also analyzed which trackers were most prevalent by entity type. Within the medical device company URL sample, the most commonly identified trackers were Google Audience (39.5%), Facebook Pixel (36.1%), and session recording (23.8%). 6.8% of the sample contained key logging trackers and 2.7% contained canvas fingerprinting.

Table 3. Most to least common banned trackers among medical device company URLs scanned (n=147).

Rank	Tracker Type	Number and Percent of URLs Containing Tracker
1	Google Audience	58 (39.5.%)
2	Facebook Pixel	53 (36.1%)
3	Session Recording	35 (23.8%)
4	Key Logging	(10 6.8%)
5	Canvas Fingerprinting	4 (2.7%)

As in the case of medical device companies, the two most frequently identified trackers in the pharmacies sample were Google Audience (28.1%) and Facebook Pixel (22.9%). Canvas fingerprinting was also identified in a fifth of the samples (20.8%), key logging in 9.4%, and session recording in 8.3%.

Table 4. Most to least common banned trackers among pharmacy URLs scanned (n=96).

Rank	Tracker Type	Number and Percent of URLs Containing Tracker
1	Google Audience	27 (28.1%)
2	Facebook Pixel	22 (22.9%)
3	Canvas Fingerprinting	20 (20.8%)
4	Key Logging	9 (9.4%)
5	Session Recording	8 (8.3%)

Within the hospital URL sample, key logging was the most frequently identified type of tracker, present on 57% of the urls scanned. Most other trackers were considerably less frequent on hospital urls than on the other two entity types, with 4.1% containing Google Audience, 3.1% containing Canvas Fingerprinting, 2% containing session recording, and 1% continuing Facebook pixel **(Table 4).**

Table 5. Most to least common banned trackers among hospital URLs scanned (n=98).

Rank	Tracker Type	Number and Percent of URLs Containing Tracker
1	Key Logging	56 (57.1.%)
2	Google Audience	4 (4.1%)
3	Canvas Fingerprinting	3 (3.1%)
4	Session Recording	2 (2%)
5	Facebook Pixel	1 (2.7%)

Discussion

McCoy et al in 2023 discussed the wider scope and legal implications of tracking technologies on hospital websites, pointing out that unauthenticated pages had at least one tracker installed. It is necessary to provide more granular analysis. The severity and impact of leaking PHI from a HIPAA covered entity depends on the type of tracker, type of data being leaked, and the type of entity. Evidence in this study suggests the use of trackers on health sites is both underreported and in violation of existing HIPAA and state privacy laws, and the severity of the violation depends on the type of tracker or use of data.

While not in the majority, it is notable that 40% of all URLs scanned had zero banned surveillance technologies installed. These sites had 0 ad trackers, no third party cookies, no fingerprinting, and

no Meta Pixel. This perhaps exemplifies that certain entities within the industry are following OCR's Guidance on trackers. Examples of clean webforms and landing pages included Fitbit, Doxy, Cleveland Clinic's Patient Portal, and Geisinger's visitpay.

Liability Risk to Health Entities

The detection of third-party tracking mechanisms on healthcare platforms class action litigation. Notably, healthcare organizations like Advocate Aurora and WakeMed have been implicated in legal disputes alleging the illicit gathering of data through Meta's tracking tool. 50 lawsuits being filed against hospital systems related to third-party tracking tech since August 2022 [14].[14] The Office of Civil Rights breach notification portal as of November 2023 showed unauthorized disclosures affecting a total of 6.1 million patients due to Meta Pixel. These breaches are now affecting millions of patients [**Table 5].**

Table 6. Examples of data breaches publicly reported 2022-2024

Name of Covered Entity	Breach Announcement	State	Individuals Affected	Breach Submission Date
CareSource	Link	OH	3,180,537	7/27/2023
Cerebral, Inc	Link	DE	3,179,835	3/1/2023
WakeMed Health and Hospitals	Link	NC	495,808	10/14/2022
Monument, Inc.	Link	NY	108,584	3/31/2023
MiniMed Distribution Corp.	Link	CA	58,374	4/14/2023
NewYork-Presbyterian Hospital	Link	NY	54,396	3/20/2023
Insulet Corporation	Link	MA	29,000	1/5/2023
UC San Diego Health	Link	CA	23,000	3/16/2023
Community Health Network, Inc. as an Affiliated Covered Entity (Notice)	Link	IN	1,500,000	11/18/2022
Novant Health Inc. on behalf of Novant Health ACE & as contractor for NMG Services Inc. (Notice)	Link	NC	1,362,296	8/14/2022
WakeMed Health and Hospitals (Notice)	Link	NC	495,808	10/14/2022
Advocate Aurora	Link	IL	3,000,000	10/14/2022
UCSF Medical Center	Link	CA	Unknown	7/25/2022
Dignity Health	Link	CA	Unknown	7/25/2022
Atrium Health Carolinas Medical Center	Link	NC	Unknown	9/20/2022
Duke University Hospital	Link	NC	Unknown	11/8/2022
Northestern Memorial	Link	IL	Unknown	10/13/2023
Costco	Link		1,000,000	10/6/2023
			14,487,638	

14 (McKeon)

Further, the utilization of third-party tracking solutions for collecting and mishandling personal information on healthcare websites can significantly undermine the confidence of patients and the broader public. This breach of trust might culminate in the diminution of patient engagement and operational revenue.

Safety Risk to Patients

Health privacy is uniquely important to protect due to the sensitive and intimate nature of the information relevant to the individual. If certain health information about an individual is exposed, this can lead to unforeseen harm and real-life consequences, including discrimination, extortion, theft, loss of employment, denial of life insurance, and potential loss of life. There are many established safety risks to patients when sensitive health data are leaked [15].[15]

The latest guidance issued by HHS clearly bans the use of tracking technologies on any health entity's public webpage about specific health conditions, including sign-up forms, registration pages, and appointment pages. In the summer of 2023, in an unprecedented joint enforcement action, HHS and the Federal Trade Commission (FTC) published letters that they sent to 130 healthcare organizations regarding the security and privacy risks of third-party tracking technology, identifying each recipient by name [16].[16] In compliance with the law, any entity using these tracking technologies is required to send Health Breach Notifications to people affected and notify the Office of Civil Rights (OCR) at HHS if 500 or more individuals are involved [17].[17]

Notable Examples

The unconsented data sharing/leakage that occurs with the use of these trackers may be harmful to patients in a variety of ways. While further research is needed to fully understand the link between certain trackers and differences in the content or ads within a patient population, the study authors are concerned about the aggressive, targeted advertising experienced by patients in this study who routinely use health-related websites on which harmful trackers were discovered. Below are examples of how patients experienced aggressive advertising on social media platforms.

- Within our dataset one of the most invasive webform was Rite Aid's sign-up form (www.riteaid.com/signup). The required fields on this form included email, username, First Name, Last Name, and Password. The page had installed a total of 48 ad trackers, fingerprinting technology designed to evade cookie blockers, and Meta Pixel. One example of a tracker used by RiteAid was Neustar. Beginning as a division of the defense contractor Lockheed Martin, Neustar provides advertisers solutions that "enhance your CRM [customer relationship management] and customer profiles with new points of contact and attributes." Their solution also allows advertisers to "Build lookalike prospect audiences with the same attributes as your top-performing customers."
- One cardiac device ID request form that had been used by a patient to enter sensitive data about their cardiac device had 17 unique ad trackers, including Microsoft Bing, and Magnite.

15 Perakslis, E.D., Ranney, M.L. & Goldsack, J.C. Characterizing cyber harms from digital health. Nat Med 29, 528–531 (2023). https://doi.org/10.1038/s41591-022-02167-6

16 https://www.ftc.gov/business-guidance/blog/2023/07/ftc-hhs-joint-letter-gets-heart-risks-tracking-technologies-pose-personal-health-information

17 45 CFR 164.408

One patient with multiple chronic conditions had previously used a webform to register her cardiac device. This patient not only reported receiving targeted ads from the device medical company on Twitter, she also reported receiving funeral ads about how to turn her body into a tree after death. We cannot determine the source of the data used to target funeral ads, and further investigation would be needed to determine a direct causal link between specific trackers and these ads.

- Members of the BRCA and Breast Cancer Community reported targeting ads for their genetic conditions,and aggressive targeting of "alternative cancer treatments" and health harming products on Meta's platform. A separate study published in May 2023 corroborated these reports, finding 310 paid advertisements from 11 alternative cancer clinics on Meta [18].[18]
- One patient with multiple chronic diagnoses, including a rare disease, was targeted with ADHD ads, autism clinical trials, cancer drugs and trials, health insurance, idiopathic hypersomnia, vaccines, skin diseases, and dialysis care on X/Twitter and Instagram.

Limitations

There are several limitations that should be understood when considering the results of the study. The team only scanned a limited sample of the hospital, pharmacy, and medical device companies that operate online in the United States. While it was important to examine some of the biggest entities in terms of revenue size (hence our selection method), we emphasize that our selection criteria do not allow inferences about the prevalence of trackers across all US hospital, pharmacy and device companies online.

Nevertheless, our results demonstrate the existence of harmful tracking technologies in health-related websites, and justifies collection of data at larger scale in a more randomized sample to reveal how many patients are exposed to this questionable practice.

Further, we were not able to scan all pages at each entity that may collect PHI and potentially contain third party trackers. Some entities may only have one page that provides opportunities for sharing PHI while others may contain multiple such pages. While the study examined frequently-visited elements of entities by prospective patients such as login portals, the team did not exhaustively examine each site for all the urls that could be associated with trackers. Thus, the results that indicate that a certain entity had no banned trackers may be true only for the specific URLs of the site that were scanned.

In addition, new surveillance technologies are continuously in development and it takes time and skill to learn how to detect them. Some surveillance technologies present on websites right now may not yet be identifiable by existing privacy scanning tools. This is an evolving area that requires ongoing efforts to identify privacy threats.

As laws and internal policies of covered entities change, so too will the use of trackers on specific links that are scanned over time. The trackers identified during the study period, for example, may have since been removed or new ones added. Further assessments may be of interest to examine how tracker use changes over time for device company, pharmacy, and hospital websites.

18 Zenone M, Snyder J, Bélisle-Pipon JC, Caulfield T, van Schalkwyk M, Maani N. Advertising Alternative Cancer Treatments and Approaches on Meta Social Media Platforms: Content Analysis. JMIR Infodemiology. 2023 May 31;3:e43548. doi: 10.2196/43548. PMID: 37256649; PMCID: PMC10267786.

Conclusion

This study demonstrates the presence of health trackers on many health-related sites despite the laws that prohibit them, and further examines the ways PHI may be shared with social media platforms or third parties via unauthenticated landing pages. Future studies are needed to assess the impact of leaking sensitive data belonging to millions of patients to third party vendors.

Despite liability risks, patient safety risks, and a definitive ban on surveillance technologies for unauthenticated webpages, this study has found significant use of tracking technologies on HIPAA Covered entities' websites between 2024-2024.

The question arises of how to address the challenge of surveillance technology on healthcare websites, given both its persistence and the grave threat it poses to citizens' privacy and well-being. Currently, the main avenue other than regulation and advisories for attempting to curb these illegal and harmful practices are individual lawsuits against entities found to be in violation. These legal efforts are critically important and are likely to result in most entities eventually removing trackers and moving into compliance with state and federal laws in an effort to avoid being the target of a lawsuit themselves. However, the authors agree with McCoy et al that "existing health privacy laws penalties may no longer be a match for the scale and nature of modern threats to patient privacy [19].[19] Every day, new threats to digital health privacy emerge and by the time lawsuits happen, harm has already been done. For that reason, the authors believe that to protect patient data proactively, a patient-led approach is required to inform new health privacy laws, new data governance standards, and a new level of patient data governance and rights.

Acknowledgements

Andrea Downing and Jill Holdren wrote the manuscript and did the primary analysis of links.

Marlena Murphy
Please include all authors' contributions, funding information, financial disclosure, role of sponsors, and other acknowledgements here. This description should include the involvement, if any, in review and approval of the manuscript for publication and the role of sponsors. Omit if not applicable.

Conflicts of Interest

None Declared.

19 McCoy MS, Friedman AB, Hoffman AK. The Scope and Legal Implications of Tracking Technologies on Hospital Websites. *JAMA.* 2023;330(3):217–218. doi:10.1001/jama.2023.8546

References

1. U.S. Department of Health & Human Services. HIPAA and Online Tracking. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.Accessed December 15, 2022.
2. Downing A, Perakslis E. Health advertising on Facebook: Privacy and policy considerations. Patterns (N Y). 2022;3(9):100561. doi:10.1016/j.patter.2022.100561.
3. Feathers T, Fondrie-Teitler S, Waller A, Mattu S. Facebook is receiving sensitive medical information from hospital websites. STAT. https://www.statnews.com/2022/06/16/facebook-meta-pixel-hospitals-data/. Published June 16, 2022. Accessed February 9, 2023.
4. Friedman AB, Merchant RM, Maley A, et al. Widespread Third-Party Tracking On Hospital Websites Poses Privacy Risks For Patients And Legal Liability For Hospitals. Health Aff (Millwood). 2023;42(4):508-515. doi:10.1377/hlthaff.2022.01205.
5. ECRI. Safety Alert.https://medcitynews.com/uploads/2022/11/ECRI-Alert-View.pdf. Published October 2022. Accessed February 4, 2023.
6. Bulletin on Online Tracking Technologies. This bulletin highlights the obligations of covered entities and business associates under the HIPAA Privacy, Security, and Breach Notification Rules when using online tracking technologies. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html. Accessed February 5, 2023.
7. “The 2022 Medtech Big 100: The world’s largest medical device companies.” Medical Design & Outsourcing, September 2022, https://www.medicaldesignandoutsourcing.com/2022-big-100/. Accessed May 2023.
8. Twenter, Paige. “15 biggest pharmacies by prescription revenue.” Becker's Hospital Review, 13 April 2023, https://www.beckershospitalreview.com/pharmacy/15-biggest-pharmacies-by-prescription-revenue.html. Accessed 14 July 2023.
9. Behm, Carly, et al. “100 largest hospitals and health systems in the US | 2023.” Becker's Hospital Review, 15 December 2023, https://www.beckershospitalreview.com/rankings-and-ratings/100-largest-hospitals-and-health-systems-in-the-us-2023.html . Accessed 12 March 2024.
10. Mattu, Surya, and Aaron Sankin. “How We Built a Real-time Privacy Inspector – The Markup.” The Markup, 22 September 2020, https://themarkup.org/blacklight/2020/09/22/how-we-built-a-real-time-privacy-inspector. Accessed 23 February 2024.
11. Englehardt S, Narayanan A. Online Tracking: A 1-million-site Measurement and Analysis. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016. https://dl.acm.org/doi/pdf/10.1145/2976749.2978313. Accessed August 10, 2023.
12. Englehardt S, Reisman D, Eubank C, Zimmerman P, Mayer J, Narayanan A, Felten EW.

Cookies That Give You Away: The Surveillance Implications of Web Tracking. In: Proceedings of the 24th International Conference on World Wide Web (Florence, Italy) (WWW '15). International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 289–299.https://doi.org/10.1145/2736277.2741679. Accessed August 10, 2023.
13. Privacy Badger. https://privacybadger.org. Accessed February 23, 2023.
14. McKeon, Jill. "Data Breach Lawsuits Tied to Tracking Pixel Use On the Rise In Healthcare." HealthITSecurity, 27 April 2023, https://healthitsecurity.com/news/data-breach-lawsuits-tied-to-tracking-pixel-use-on-the-rise-in-healthcare. Accessed 12 March 2024.
15. Perakslis ED, Ranney ML, Goldsack JC. Characterizing cyber harms from digital health. Nat Med. 2023;29:528–531. doi:10.1038/s41591-022-02167-6.
16. Fair L. FTC-HHS joint letter gets to the heart of the risks tracking technologies pose to personal health information.https://www.ftc.gov/business-guidance/blog/2023/07/ftc-hhs-joint-letter-gets-heart-risks-tracking-technologies-pose-personal-health-information. Published July 20, 2023. Accessed August 10, 2023.
17. 45 CFR 164.408. Notification to the Secretary. In: Electronic Code of Federal Regulations Title 45. https://www.govinfo.gov/app/details/CFR-2018-title45-vol1/CFR-2018-title45-vol1-sec164-408/summary. Updated as of February 14, 2024. Accessed Feb 15, 2024.
18. Zenone M, Snyder J, Bélisle-Pipon JC, Caulfield T, van Schalkwyk M, Maani N. Advertising Alternative Cancer Treatments and Approaches on Meta Social Media Platforms: Content Analysis. JMIR Infodemiology. 2023;3:e43548. doi:10.2196/43548.
19. McCoy MS, Friedman AB, Hoffman AK. The Scope and Legal Implications of Tracking Technologies on Hospital Websites. JAMA. 2023;330(3):217–218. doi:10.1001/jama.2023.8546.

Abbreviations

1. **URL - Uniform Resource Locator:** A reference or address to a resource on the Internet, specifying the location of a web page or resource on a network.
2. **PHI - Protected Health Information:** Information in a medical record or other health-related information that can be used to identify an individual, which was created, used, or disclosed in providing healthcare services.
3. **ECRI - Emergency Care Research Institute:** A nonprofit organization that researches approaches to improving patient care. (Note: While ECRI stands for Emergency Care Research Institute, it is now known simply as ECRI to reflect a broader scope beyond emergency care.)
4. **HHS - U.S. Department of Health & Human Services**: The United States government's principal agency for protecting the health of all Americans and providing essential human services.
5. **OCR - Office for Civil Rights:** A division within the U.S. Department of Health and Human Services that enforces civil rights laws, as well as privacy and security laws related to healthcare information.
6. **FTC - Federal Trade Commission:** An independent agency of the United States government, whose principal mission is the enforcement of civil U.S. antitrust law and the promotion of consumer protection.
7. **HIPAA - Health Insurance Portability and Accountability Act:** United States legislation that provides data privacy and security provisions for safeguarding medical information.
8. **CRM**: Customer Relationship Management. Many marketing “CRM” tools use surveillance technologies.